AMENDMENTS TO THE CLAIMS

Following is a listing of all claims in the present application, which listing supersedes all previously presented claims:

Listing of Claims:

1. (Currently Amended) A cryptographic method using dual keys in a wireless local area network (LAN) system, comprising:

(a) generating a first group key in N wireless terminals forming an ad-hoc group, where N is equal to or greater than two;

(b) generating an initial second group key in a main wireless terminal to perform a key distribution center function among the N wireless terminals in response to a request from one of (N-1) sub wireless terminals, the request being communicated using the first group key, and transmitting the initial second group key to (N-1) sub wireless terminals;

(c) encoding data using the initial second group key, and transmitting the encoded data between the N wireless terminals;

(d) modifying the initial second group key in the main wireless terminal according to a modification time period to form at least one modified second group key, the modification time period being predetermined in the main wireless terminal; and

(e) transmitting the at least one modified second group key to the (N-1) sub wireless terminals, wherein the at least one modified second group key is transmitted and used to encode data between the N wireless terminals during use of the first group key, wherein in (e), the at least one modified second group key is encoded using the initial second group key, the method further comprising transmitting the encoded modified second group key to the (N-1) sub wireless terminals,

wherein in (b), the main wireless terminal encodes the initial second group key using the first group key, and transmits the encoded initial second group key to the (N-1) wireless terminals.

2. (Original) The method as claimed in claim 1, wherein the first group key is generated using a group password of the ad-hoc group.

3. (Cancelled)

4. (Original) The method as claimed in claim 1, wherein the main wireless terminal is a creator of the ad-hoc group.

5. (Previously Presented) The method as claimed in claim 1, wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers the key distribution center function to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

6.-7. (Canceled).

8. (Previously Presented) The method as claimed in claim 1, wherein (b) comprises:

(b1) when the first group key is created, encoding a second group key request message from one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request message to the main wireless terminal;

(b2) decoding the second group key request message, using the first group key, in the main wireless terminal; and

(b3) creating the initial second group key according to the decoded second group key request message, in the main wireless terminal.

9. (Previously Presented) A tangible computer readable medium having embodied thereon a computer program for the method according to claim 1.

10. (Currently Amended) A tangible computer readable medium having embodied thereon a computer program for the method according to claim [[3]] 5.

11. (Previously Presented) A tangible computer readable medium having embodied thereon a computer program for the method according to claim 8.

12. (Currently Amended) A wireless local area network (LAN) system, comprising:

N, where N is equal to or greater than two, wireless terminals which form an ad-hoc group, and create first and second group keys, wherein the N wireless terminals include:

a main wireless terminal for performing a key distribution center function in the ad-hoc group, for creating an initial second group key in response to a request from one of (N-1) sub wireless terminals, the request being communicated using the first group key, and encoding data using the initial second group key, and for transmitting the encoded data between the remaining wireless terminals; and

(N-1) sub wireless terminals for generating a first group key and for receiving the initial seond group key from the main wireless terminal and encoding data using the initial

second group key, and for transmitting the encoded data between the remaining wireless terminals,

wherein the main wireless terminal modifies the initial second group key according to a modification time period to form at least one modified second group key, the modification time period being predetermined in the main wireless terminal;

wherein the main wireless terminal transmits the at least one modified second group key to each of the (N-1) sub wireless terminals, the at least one modified second group key being transmitted and used to encode data between the N wireless terminals during use of the first group key; [[and]]

wherein the main wireless terminal encodes the initial second group key using the first group key, and transmits the encoded initial second group key to the (N-1) wireless terminals; and

wherein the main wireless terminal encodes the at least one modified second group key using the initial second group key, and transmits the encoded modified second group key to the (N-1) sub wireless terminals.

13. (Original) The system as claimed in claim 12, wherein the first group key is generated using a group password of the ad-hoc group.

14. (Cancelled)

15. (Original) The system as claimed in claim 12, wherein the main wireless terminal is a creator of the ad-hoc group.

16. (Previously Presented) The system as claimed in claim 12, wherein when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers the key distribution center function to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

17. (Previously Presented) The system as claimed in claim 12, wherein each sub wireless terminal comprises:

a first group key generator for creating the first group key using a group password input from a user;

a first encryption unit for storing the first group key, for encoding a second group key request message using the first group key, for decoding a second group key response message from the main wireless terminal using the first group key, and for encoding data input from a user using the modified second group key; and

a first key management unit for generating the second group key request message to output to the first encryption unit, for extracting the initial second group key from the second group key response message decoded in the first encryption unit, and for outputting the extracted initial second group key to the first encryption unit.

18. (Previously Presented) The system as claimed in claim 17, wherein the main wireless terminal comprises:

a second group key generator for creating the first group key using a group password input from a user;

a second encryption unit for storing the first group key, for decoding the second group key request message transmitted from the sub wireless terminal using the first group key, for

encoding the second group key response message for transmitting to the sub wireless terminal using the first group key, and for encoding data input from a user using the initial second group key; and

a second key management unit for receiving the second group key request message decoded from the second encryption unit, for creating the initial second group key, and for outputting the second group key response message including the created initial second group key to the second encryption unit.

19. (Canceled).

20. (Previously Presented) The system as claimed in claim 18, wherein the second encryption unit encodes the modified second group key using the initial second group key, and transmits the encoded modified second group key to each of the (N-1) sub wireless terminals.

21. (Currently Amended) A wireless terminal using dual keys for cryptography, the wireless terminal for performing a key distribution center function in an ad-hoc group including other wireless terminals, the wireless terminal comprising:

first means for creating an initial second group key in accordance with a first group key, for encoding data using the initial second group key, for transmitting the encoded data between the other wireless terminals, for modifying the initial second group key according to a predetermined modification time period to form at least one modified second group key, and for transmitting the at least one modified second group key to at least one wireless terminal,

wherein the at least one modified second group key is transmitted and used to encode data during use of the first group key, [[and]]

wherein the wireless terminal encodes the initial second group key using the first group key, and transmits the encoded initial second group key to the other wireless terminals; and

wherein the wireless terminal encodes the at least one modified second group key using the initial second group key, and transmits the encoded modified second group key to other wireless terminals.

22. (Currently Amended) The wireless terminal as claimed in claim 25, wherein the encryption unit encodes the at least one modified second group key using the initial second group key, and transmits the encoded modified second group key to the at least one wireless terminal via the encryption unit.

23. (Currently Amended) A wireless terminal using dual keys for cryptography, the wireless terminal comprising:

first means for creating a first group key, for receiving an initial second group key communicated using the first group key and a modified second group key, communicated using the initial second group key from another wireless terminal performing a key distribution center function in an ad-hoc group, for encoding data using the modified second group key, and for transmitting the encoded data between wireless terminals existing in the ad-hoc group,

wherein the initial second group key is modified in the other wireless terminal performing the key distribution center according to a predetermined modification time period to form the at least one modified second group key,

wherein at least one modified second group key is transmitted and used to encode data during use of the first group key, [[and]]

wherein the wireless terminal encodes the initial second group key using the first group key, and transmits the encoded initial second group key to the other wireless terminals; and

wherein the wireless terminal encodes the at least one modified second group key using the initial second group key, and transmits the encoded modified second group key to the other wireless terminals.

24. (Previously Presented) The wireless terminal as claimed in claim 23, wherein the first means comprises:

a group key generator for creating the first group key;

an encryption unit for encoding a second group key request message using the first group key, for decoding a second group key response message using the first group key, and for encoding data input from a user using the modified second group key; and

a key management unit for generating the second group key request message to output to the encryption unit, for extracting the initial second group key from the decoded group key response message, and for outputting the extracted initial second group key to the encryption unit.

25. (Previously Presented) The wireless terminal as claimed in claim 21, wherein the first means comprises:

a group key generator for creating the first group key;

an encryption unit for encoding a second group key response message corresponding to a second group key request message transmitted from the at least one wireless terminal

using the first group key, for transmitting the encoded second group key response message to the at least one wireless terminal, and for encoding data input from a user using the modified second group key; and

a key management unit for receiving the second group key request message, for creating the initial second group key, for outputting the second group key response message including the created initial second group key to the encryption unit, and for modifying the initial second group key according to the predetermined modification time period.